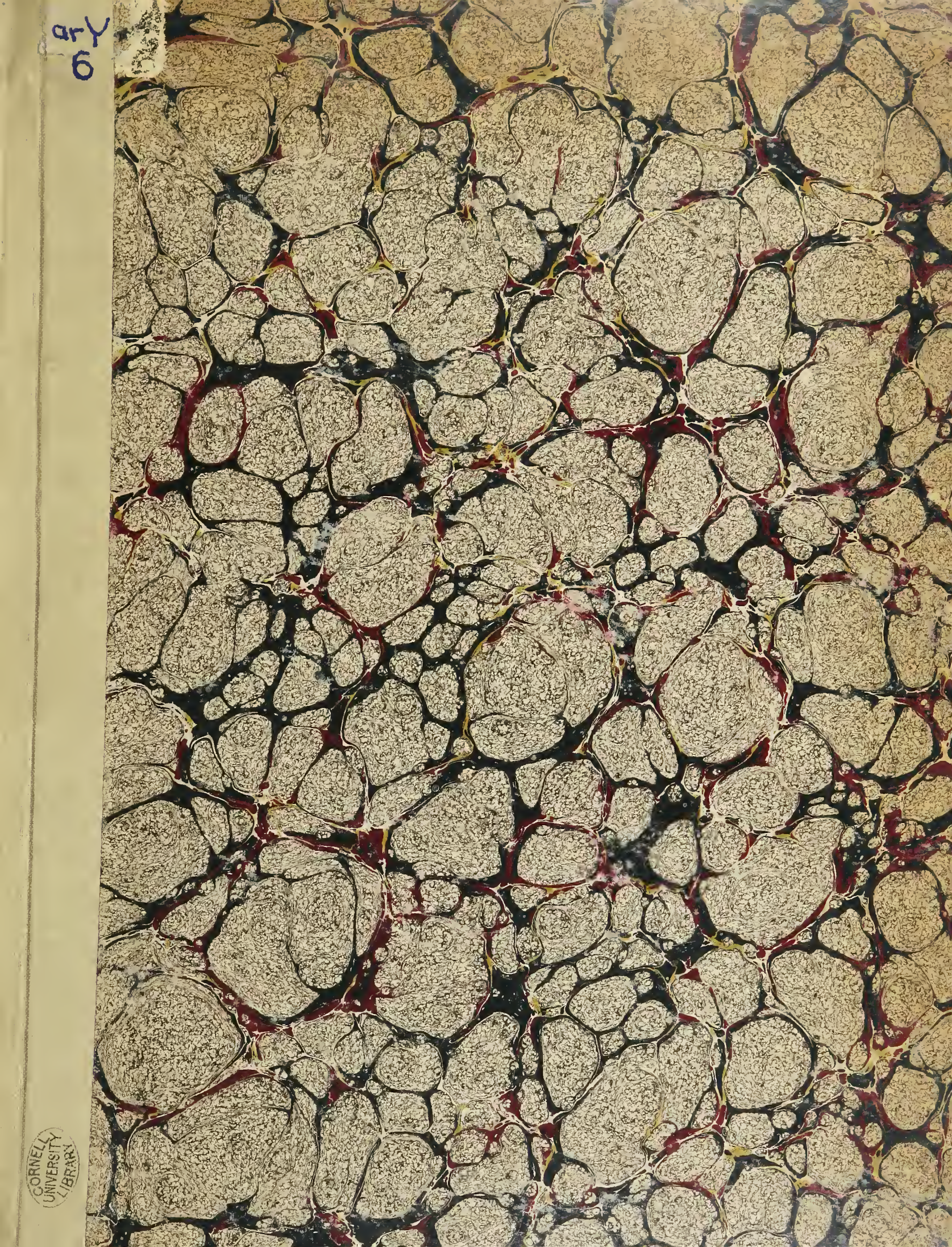

ON PRIMITIVE GROUPS OF ODD ORDER

A THESIS

PRESENTED TO THE UNIVERSITY FACULTY OF CORNELL UNIVERSITY IN CANDIDACY FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

HENRY LEWIS RIETZ

BALTIMORE
The Lord Baltimore Press
THE FRIEDENWALD COMPANY
1904

ON PRIMITIVE GROUPS OF ODD ORDER

A THESIS

PRESENTED TO THE UNIVERSITY FACULTY OF CORNELL UNIVERSITY IN CANDIDACY FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

BY

HENRY LEWIS RIETZ

BALTIMORE
The Lord Baltimore Press
THE FRIEDENWALD COMPANY
1904

On Primitive Groups of Odd Order.

By Henry Lewis Rietz.

Introduction.

In his "Theory of Groups of Finite Order" (1897), p. 379, Burnside has called attention to the fact that no simple group of odd composite order is known to exist. Several articles* have recently appeared bearing on this question, in which, among other things, it was proved that no such group can be represented as a substitution group whose degree does not exceed 100. This result was obtained by showing that there is no simple primitive group of odd composite order whose degree falls within the given limits. Burnside determined all the primitive groups of odd order of degree less than 100.†

Since any primitive group of odd order is simply transitive, a study of simply transitive primitive groups may throw light on the question of simple groups of odd order. Some important properties of simply transitive primitive groups have been given by Jordan, Miller, and Burnside.‡

The main objects of the present paper are; first, to make a further study of primitive groups with special reference to those of odd order; secondly, to extend the determination of the primitive groups of odd order to all degrees less than 243.

It results that all groups arrived at in this determination are solvable. From this result it is evident that no simple group of odd composite order can occur

* Miller, Proc. Lond. Math. Soc., Vol. 33, pp. 6–10. Burnside, Proc. Lond. Math. Soc., Vol. 33, pp. 162–185; 257–268. Frobenius, Berliner Sitzungsberichte (1901), pp. 849–858; 1216–1230.

† At the time of the publication of this work, I had also made this determination with the same results.

‡ Jordan, "Traité des Substitutions," pp. 281–284. Miller, Proc. Lond. Math. Soc., Vol. 28, pp. 533–542. Burnside, loc. cit., pp. 162–185.

as a substitution group of degree less than 243, since if a simple group is represented as a substitution group on the minimum number of letters, it is primitive.

Part I contains a number of theorems, most of which apply to primitive groups whether the order is even or odd, but some use can be made of nearly all of them in determining all the primitive groups of odd order of a given degree. Part II contains the determination of the primitive groups of odd order whose degrees lie between 100 and 243.

I desire to acknowledge my indebtedness to Professor G. A. Miller for helpful suggestions and criticisms during the preparation of this paper.

PART I.

§1.—*On the Number of Substitutions of Degree less than n contained in any Transitive Group of Degree n.*

Let G be any primitive group of composite order g on the elements $a_1, a_2, \ldots, a_n$, and G_s the subgroup leaving a given letter a_s fixed. If $n - \lambda_\alpha$ is the degree of any substitution of G_s, and μ_α the number of substitutions of G_s of this degree, then the total number of substitutions of degree less than n contained in G is

$$\frac{n\mu_1}{\lambda_1} + \frac{n\mu_2}{\lambda_2} + \frac{n\mu_3}{\lambda_3} + \ldots + \frac{n\mu_\rho}{\lambda_\rho}^* \quad \text{or} \quad n\left(\frac{\mu_1}{\lambda_1} + \frac{\mu_2}{\lambda_2} + \frac{\mu_3}{\lambda_3} + \ldots + \frac{\mu_\rho}{\lambda_\rho}\right),$$

where ρ is the number of different degrees occurring among the substitutions of G_s. Since $\mu_1 + \mu_2 + \mu_3 + \ldots + \mu_\rho = \frac{g}{n}$, the above summation in the parentheses may be considered as the sum of just $\frac{g}{n}$ terms of the form $\frac{1}{\lambda}$. We may then rewrite the above expression for the number of substitutions of degree less than n in the form

$$n \sum_{\alpha=1}^{\alpha=\frac{g}{n}} \frac{1}{\lambda_\alpha}. \tag{1}$$

Let x denote the number of systems of intransitivity of G_s, and look upon G_s as having just one system of intransitivity when it is transitive. Then $x + 1$

---

* Jordan, Liouville's Journal, Vol. 17 (1872), p. 352.

is the average value of λ_α since the average number of letters in the substitutions of an intransitive group is equal to the excess of the degree over the number of systems of intransitivity.* Hence we have

$$x + 1 = \frac{\sum_{\alpha=1}^{\alpha=\frac{g}{n}} \lambda_\alpha}{\frac{g}{n}}. \tag{2}$$

The λ's in this summation cannot all be equal, since identity is included among the substitutions of G_s. Since the arithmetic mean of any number of positive quantities which are not all equal is greater than their geometric mean, it follows that

$$\frac{\sum_{\alpha=1}^{\alpha=\frac{g}{n}} \lambda_\alpha}{\frac{g}{n}} > \sqrt[\frac{g}{n}]{\lambda_1 \lambda_2 \ldots \lambda_{\frac{g}{n}}} \tag{3}$$

and

$$\frac{\sum_{\alpha=1}^{\alpha=\frac{g}{n}} \frac{1}{\lambda_\alpha}}{\frac{g}{n}} > \sqrt[\frac{g}{n}]{\frac{1}{\lambda_1} \cdot \frac{1}{\lambda_2} \cdots \frac{1}{\lambda_{\frac{g}{n}}}}. \tag{4}$$

From (3) and (4) it follows that

$$\frac{\left(\frac{g}{n}\right)^2}{\sum_{\alpha=1}^{\alpha=\frac{g}{n}} \lambda_\alpha} < \sum_{\alpha=1}^{\alpha=\frac{g}{n}} \frac{1}{\lambda_\alpha}. \tag{5}$$

From (2) and (5) it follows that

$$\frac{g}{n(x+1)} < \sum_{\alpha=1}^{\alpha=\frac{g}{n}} \frac{1}{\lambda_\alpha} \quad \text{or} \quad \frac{g}{x+1} < n \sum_{\alpha=1}^{\alpha=\frac{g}{n}} \frac{1}{\lambda_\alpha}. \tag{6}$$

---

* Jordan, Comptes Rendus, Vol. 74 (1872), p. 977. Frobenius, Crelle's Journal, Vol. 101 (1887), p. 288.

From (1) and (6) we obtain

THEOREM 1.—*In any primitive group G of degree n of composite order g there are more than $\frac{g}{x+1}$ substitutions of degree less than n, where x is the number of systems of intransitivity of the subgroup which leaves a given letter fixed.*

In particular, for a multiply transitive group, $x = 1$. Hence,

Cor. 1. *In a multiply transitive group of degree n more than one-half of the substitutions are of degree less than n.*

Cor. 2. *If G is of degree kp (p a prime) and of order mp (m prime to p and $p-1$), the subgroup G_s has at least $p+1$ transitive constituents.*

For a group of this order contains exactly m operators whose orders divide m.* But all the substitutions of degree less than kp would be of orders prime to p. Hence from the above theorem we have $x > \frac{mp}{x+1}$ or $x > p-1$.

Since mp must clearly be an odd number, x must be even. Hence, $x \geqq p+1$.

While it is not our object to treat imprimitive groups, the above theorem can at once be extended to any non-regular transitive group. The only change in the argument is the substitution of $x+m$ in expression (1) for $x+1$, where m represents the number of letters of the transitive group left fixed by the subgroup which leaves a given letter fixed. Hence,

THEOREM 2.—*In any non-regular transitive group of degree n of order g there are more than $\frac{g}{x+m}$ substitutions of degree less than n, where x and m are defined as above.*

When applied to known groups, I find that in many cases this simple formula gives very nearly the actual number of substitutions of degree less than the degree of the group.

---

* Frobenius, Berliner Sitzungsberichte (1895), p. 1035.

§2.—*Restrictions on the Order of G, when G_s has a Transitive Constituent of Degree p, p^α, pm or pq (p and q primes and $m < p$).*

If G is simply transitive, G_s is intransitive and conversely. Use will frequently be made of the following known theorems:

1. If G_s contains an invariant subgroup H_s of degree $n - \alpha$, H_s is intransitive, and of the n conjugates to which it belongs under G just $\alpha - 1$, besides $H_s (H_{s_1}, H_{s_2}, \ldots, H_{s_{\alpha-1}})$ occur in G_s. These $\alpha - 1$ subgroups generate a group of degree $n - 1$. Furthermore, G_s transforms $H_{s_1}, H_{s_2}, \ldots, H_{s_{\alpha-1}}$ in the same manner as the elements of one of its constituent groups are permuted.*

2. Every prime which divides the order of one transitive constituent of G_s divides the order of each of its constituents.†

THEOREM 3.—*If in G_s all the transitive constituents $T_1, T_2, T_3, \ldots$ of a given degree t are of orders $s_1, s_2, s_3, \ldots$, and if $\frac{s_1}{t}, \frac{s_2}{t}, \frac{s_3}{t}, \ldots$ do not contain a given prime p occurring as a factor in t, the order of G_s is of the form tk, where k is prime to p.*

We shall assume that the invariant subgroup H_s of G_s corresponding to identity in T_1 is of order $h = \lambda p^m$ (λ prime to p, $m > 0$); this must be the case if the theorem is not true. It will be shown that this hypothesis leads to a contradiction. In H_s all the substitutions whose orders are powers of p would generate a group H_s' of order $\lambda' p^m$ invariant in G_s. In the conjugate G_r of G_s, leaving fixed an element of T_1, there occurs just $1/t$ of the substitutions of G_s. Hence the subgroup H_s' would be one of a set of t conjugates transformed by G_r according to one of its transitive constituents T' of degree t. In the invariant subgroup H_r' of G_r corresponding to identity in T', all the substitutions are common to G_r and G_s, since they transform H_s' into itself. Now H_r' would be of order $\lambda'' p^m$ (λ'' prime to p). Since in T_1 all the substitutions whose orders are not prime to p are of degree t, all the substitutions whose orders are powers of p common to G_r and G_s are contained in H_s.

If H_r' contained all the substitutions whose orders are powers of p which occur in H_s, the subgroup H_s' would be invariant in G_s and G_r. But this is impossible, since these subgroups are maximal. If H_r' contains only part of these substitutions, let P be such a substitution not contained in H_r'. The order of

* Miller, loc. cit., pp. 534, 535. † Jordan, loc. cit., p. 284.

$\{H_r', P\}$ would then be divisible by p^{m+1} and there would be common to G_s and G_r subgroups of order p^{m+1}, which is impossible, since, by hypothesis, the order of H_s is not divisible by p^{m+1}. Hence the theorem.

Cor. 1. *If G_s has a transitive constituent of prime degree p, the order of G_s is not divisible by p^2.*

Cor. 2. *If any number of the transitive constituents of H_s are of a given prime degree p, the constituent group formed of all these transitive constituents is formed by establishing a simple isomorphism between them.*

Cor. 3. *If in G_s all the transitive constituents of a given degree p^α are of class $p^\alpha - 1$, the order of G_s is not divisible by $p^{\alpha+1}$.*

Cor. 4. *If in G_s all the transitive constituents of degree $mp\,(p > m)$ have p systems of imprimitivity, the order of G_s is not divisible by p^2.*

Lemma. When p and q are distinct primes each of the form $2^m + 1$, there is no imprimitive group of degree pq of odd order whose order is divisible by both p^2 and q^2; and there is no primitive group of degree pq involving in its order only the primes p and q.

The part of this lemma which relates to the imprimitive groups follows at once from the fact, that the only transitive groups of degrees p and q whose orders are odd are the cyclical groups of orders p and q. Suppose there is a primitive group of degree pq of order $p^{\alpha_1}q^{\alpha_2}$. The maximal subgroup G_1, leaving a given letter fixed, is then of degree $pq - 1$ and of order $p^{\alpha_1-1}q^{\alpha_2-1}$. Take $p > q$, then, since $p^2 > pq - 1$, no transitive constituent can be of degree $p^\gamma (\gamma > 1)$. The transitive constituents cannot all be of degree p, since p is not a divisor of $pq - 1$. Since $pq - 1$ is not divisible by q, we may assume that some of the transitive constituents are of degree p while others are of degrees equal to a power of q. But the order of a transitive constituent of degree p is p, and would therefore not contain q as a factor, but every prime which divides the order one transitive constituent of G_1 divides the order of each of its transitive constituent.

THEOREM 4.—*If p and q are distinct primes of the form $2^m + 1$, and if G_s is of odd order, and has as a transitive constituent an imprimitive group of degree pq; then, according as T has p or q systems of imprimitivity, the order of G_s is not divisible by p^2 or q^2.*

To make the conditions definite, suppose that T has q systems of imprimitivity. These systems are then permuted according to the cyclical group of

order q, and all the substitutions in the tail of T are of degree pq. Corresponding to identity in T, there is in G_s an invariant subgroup H_s of degree $n - \alpha\,(\alpha \leqslant pq + 1)$. If we can show that the order of H_s is not divisible by q, our theorem is proved. Let G_r be the conjugate of G_s which leaves fixed an element of T. Also let R_s be the invariant subgroup of G_s corresponding to the head of T. In G_r the subgroup H_s is one of a set of pq conjugates transformed by G_r according to a transitive constituent T_1 of order $p^{\alpha_1}q^{\alpha_2}$. According to the lemma, T_1 is imprimitive and its order is not divisible by both p^2 and q^2. The subgroup T_1, leaving a given letter fixed, would leave more than one letter fixed. Hence in G_r the subgroup H_s is transformed into itself by some of its conjugates. Let H_{s_1} be one of these conjugates such that $H_{s_1}^{-1}H_sH_{s_1} = H_s$. H_{s_1} then occurs in both G_s and G_r. Hence, it occurs in R_s. If R_s contains operators of order q, they clearly occur in H_s. Hence, H_s and H_{s_1} have the same substitutions of order q. But H_s is invariant in G_s and H_{s_1} in G_{s_1}. The substitutions of order q in H_s would then generate a group invariant in both G_s and G_{s_1}. But this is impossible, since G_s is maximal. Hence the theorem.

§3.—*On Certain Subgroups Contained in G.*

Let p^α be the highest power of a prime p which divides the order of G, and suppose that the number p is prime to n, the degree of G. Let P be any subgroup of order p^α. It must be contained in some of the subgroups $G_1, G_2, \ldots, G_n$, leaving a given letter fixed, since its degree is prime to n. If P is of degree $n - \lambda\,(\lambda > 1)$, it is proved by Burnside ("Theory of Groups," p. 202), that the subgroup of G, which contains all the substitutions of G which transform P into itself, permutes the λ elements not occurring in P transitively. It is our object to consider the case $\lambda = 1$. Let P' be a subgroup of order p^β common to any two of the subgroups $G_1, G_2, G_3, \ldots, G_n$ such that there is no subgroup of order $p^\gamma\,(\gamma > \beta)$ common to any two of these subgroups. We shall first assume $\beta > 0$. P' must be contained in subgroups P_1 and P_2 of order p^α in those subgroups which leave a given letter fixed in which it occurs. Since, in a subgroup of order p^α, any subgroup P' is transformed into itself by operators of the group not contained in P', it follows that P' is invariant in a subgroup P'' of P_1 which is of degree $n - 1$. Likewise in P_2 the subgroup P' is invariant in a subgroup P''' of degree $n - 1$. Hence, the subgroup P' is invariant in $\{P'', P'''\}$

of degree n. Since $n \equiv 1 \bmod p$, the number of elements of G not occurring in P' is congruent to unity mod p. Also, since P'' and P''' are each of degree $n-1$, it follows that $\{P'', P'''\}$ has a transitive constituent of degree $1+kp$ $(k>0)$, formed of elements not occurring in P', and whose order is multiple of p.

When $\beta = 0$, the subgroup P is clearly formed by establishing a simple isomorphism between regular groups. Hence,

THEOREM 5.—*If p^α is the highest power of a prime p which divides the order of G, and if a subgroup P of order p^α is of degree $n-1$, then, unless P is a regular group or is formed by establishing a simple isomorphism between regular groups of order p^α, G contains an intransitive subgroup of degree n having a transitive constituent of degree $1+kp$ $(k>0)$ and of order lp.*

Cor. *If p^α is the highest power of a prime p which divides the order of G_s, and if the degree of each transitive constituent of G_s is divisible by p^β, but at least one of them is not divisible by $p^{\beta+1}$, then either $\alpha = \beta$ or the group G contains a subgroup of degree n having a transitive constituent of degree $1+kp$ $(k>0)$ and of order equal to a multiple of p.*

It may be observed that the theorem and corollary just stated apply to any transitive group in which the subgroup which leaves a given letter fixed leaves only one letter fixed, as well as to a primitive group.

§4.—*On the Transitive Constituents of G_s.*

THEOREM 6.—*If G_s has an invariant subgroup H_s of degree $n-\alpha$ $(\alpha>1)$, then G_s has at least one transitive constituent whose degree exceeds the degree of any transitive constituent of H_s.*

Suppose, if possible, that H_s has a transitive constituent T such that its degree is equal to the degree of the transitive constituents of G_s of largest degree.

Consider a conjugate G_r of G_s, leaving fixed an element of G_s not occurring in H_s. Since H_s occurs in both G_s and G_r, these two groups have at least one transitive constituent in the same elements, i. e., in the elements of T. The group $\{G_r, G_s\}$ would then be intransitive. But $\{G_r, G_s\}$ must be identical

with G, since G_s is maximal. Hence the hypothesis that H_s has the transitive constituent T leads to an absurdity.

Cor. *If all the transitive constituents of G_s are primitive groups of the same degree t, then G_s is formed by establishing a simple isomorphism between these transitive constituents.*

This follows readily from the theorem if we remember that every invariant subgroup of a primitive group is transitive.

THEOREM 7.—*If G_s has as a transitive constituent a regular group T of degree t, and if the order of G_s exceeds t, then G_s has another transitive constituent of degree t which has the property that its subgroup which leaves a given letter fixed permutes all the remaining letters.*

Consider the invariant subgroup H_s of G_s corresponding to identity in T. In a conjugate H_r of G_s, leaving fixed an element of T, there occur just $1/t$ of the substitutions of G_s and the subgroup H_s is one of t conjugates transformed according to a transitive constituent T_1. If, in the group T_1, the subgroup which leaves a given letter fixed, leaves more than one letter fixed, H_s is transformed into itself by some of its t conjugates under G_r. But the substitutions of H_s are the only substitutions common to G_r and G_s. Hence, the transitive constituent T_1 has the property mentioned in the theorem.

THEOREM 8.—*If G_s has λ systems of intransitivity, and if H_s is the invariant subgroup of G_s corresponding to identity in any transitive constituent T, while G_s transforms $H_{s_1}, H_{s_2}, \ldots, H_{s_{\alpha-1}}$* (defined as in §2) *according to a constituent group having μ systems of intransitivity, then H_s has more than $\frac{\lambda}{\mu}$ systems of intransitivity, excepting when $\mu = 1$, and then it has at least λ.**

If H_s has as few as $\frac{\lambda}{\mu}$ systems of intransitivity, the μ conjugate sets under G_s into which $H_{s_1}, H_{s_2}, \ldots, H_{s_{\alpha-1}}$ are divided could, at most, contain elements from $\left(\frac{\lambda}{\mu} - 1\right)\mu + 1 = \lambda - \mu + 1$ of the λ systems of intransitivity of G_s, since each of the subgroups $H_{s_1}, H_{s_2}, \ldots, H_{s_{\alpha-1}}$ must contain at least a cycle from T.

* Cf. Miller, loc. cit., p. 535

These subgroups could not then generate a group of degree $n-1$ unless $\mu = 1$. Hence, by means of 1, §2, the theorem follows.

Cor. *If all the transitive constituents of* G_s *are primitive groups,* $H_{s_1}, H_{s_2}, \ldots, H_{s_{\alpha-1}}$ *cannot be a single conjugate set under* G_s.

§5.—*On the Transitive Constituents of* G_s *when the Order of* G *is Restricted to be an Odd Number.*

Burnside recently proved the interesting theorem* that, if G is of odd order, G_s has its transitive constituents in pairs of the same degree.

Let $a_{s_1}, a_{s_2}, a_{s_3}, \ldots, a_{s_t}$ be the elements of any transitive constituent of degree t. The above theorem was proved by considering the quadratic function

$$f = \sum_{s=1}^{s=n} a_s (a_{s_1} + a_{s_2} + \ldots + a_{s_t}),$$

which is transformed into itself by all the substitutions of G. In this summation, a_s occurs in the parentheses exactly t times. Hence the function f may also be written

$$f = \sum_{s=1}^{s=n} (a_{s_1'} + a_{s_2'} + \ldots + a_{s_t'})\, a_s,$$

and it is shown in the proof of the above theorem that the elements $a_{s_1'}, a_{s_2'}, a_{s_3'}, \ldots, a_{s_t'}$ are elements of a transitive constituent T' of G_s distinct from T. The constituents T and T' will be spoken of as a "pair of transitive constituents." Use will be made of the two ways in which f is written to prove some theorems in reference to the transformation by G_s of its subgroups $H_{s_1}, H_{s_2}, \ldots, H_{s_{\alpha-1}}$ (defined as in §2) when H_s corresponds to identity in T. It is known (p. 5) that these $\alpha - 1$ subgroups are transformed by G_s according to one of its constituent groups. But it is not known whether this constituent group ever contains elements occurring in H_s. Form the conjugate G_{s_α} of G_s, leaving fixed an element of T. From the two ways of writing f, it is seen that in G_{s_α} the element a_s occurs in the transform of T'; i. e., in $R^{-1}T'R$, where R is such that $R^{-1}G_sR = G_{s_\alpha}$. But H_s is transformed by G in the same manner as a_s is replaced. Hence,

---

* Loc. cit., p. 163.

THEOREM 9.—*Some of the subgroups* $H_{s_1}, H_{s_2}, \ldots, H_{s_{\alpha-1}}$ *are transformed according to* T' *when* H_s *corresponds to identity in* T.

Cor. *If the subgroups* $H_{s_1}, H_{s_2}, \ldots, H_{s_{\alpha-1}}$ *are a single conjugate set under* G_s, *they are transformed according to* T' *when* H_s *corresponds to identity in* T.

Suppose, next, that G_s has only two transitive constituents T' and T. If, corresponding to identity in one of these constituents, say T, there is in G_s an invariant subgroup H_s, the subgroups $H_{s_1}, H_{s_2}, \ldots, H_{s_{\frac{n-1}{2}}}$ (Cor., Theor. 9) are transformed by G_s according to the elements of H_s. Then, for any two of the n subgroups $H_1, H_2, \ldots, H_n$, which are conjugate under G, one of two relations

$$H_\beta^{-1} H_\alpha H_\beta = H_\alpha \quad \text{or} \quad H_\alpha^{-1} H_\beta H_\alpha = H_\beta \tag{1}$$

holds, but both cannot hold for any two of the subgroups. Let x be the number of elements common to H_α and H_β; then x is clearly the number of elements common to any two of the H's. Also, let $x + y$ be the degree of H_s. Let $a_1, a_2, \ldots, a_y, b_1, b_2, \ldots, b_x$ be the elements of H_s, and $b_1, b_2, \ldots, b_x, c_1, c_2, \ldots, c_y$ the elements of H_{s_1}, one of the subgroups $H_{s_1}, H_{s_2}, \ldots, H_{s_{\frac{n-1}{2}}}$ contained in G_s. Since H_{s_1} must be transformed according to an element of H_s not contained in H_{s_1}, it must be transformed according to one of the a's. There must be substitutions in H_s which do not transform H_{s_1} into itself. If S is such a substitution, then $S^{-1} H_{s_1} S$ contains all the a's, since H_{s_1} and $S^{-1} H_{s_1} S$ have just x elements in common. But since a_{s_1}, according to which H_{s_1} is permuted, occurs in $S^{-1} H_{s_1} S$, this latter subgroup cannot transform H_{s_1} into itself. By exactly the same reasoning H_{s_1} cannot transform $S^{-1} H_{s_1} S$ into itself. But this is contrary to relations (1). Hence,

THEOREM 10.—*If, in a primitive group* G *of odd order, the subgroup* G_s *has only two transitive constituents,* G_s *is formed by establishing a simple isomorphism between them.*

THEOREM 11.—*If, in a primitive group* G *of odd order,* G_s *has not more than four transitive constituents, and if these are all primitive groups, then it is formed by establishing a simple isomorphism between them.*

Since G_s has an even number of transitive constituents, we need consider only the cases where it has two or four transitive constituents. Since any invariant subgroup of a primitive group is transitive, and since a simply transitive

primitive group of degree n cannot have a transitive subgroup of degree less than n, the theorem follows at once when G_s has only two transitive constituents.

If G_s has four transitive constituents, and is not formed according to the theorem, there corresponds to identity in some transitive constituent T of degree t an intransitive subgroup H_s invariant in G_s. It has two or three systems of intransitivity. Suppose, first, that H_s of degree $n-\alpha$ has three systems. Then $\alpha - 1 = t$. In the conjugate of G_s, leaving fixed a letter of T, the subgroup H is one of t conjugates. But these $\alpha - 1$ subgroups cannot be conjugate (Cor., Theor. 8). It remains to consider the case where H_s has two systems of intransitivity; then $n-\alpha$ (the degree of H_s) is an even number. Hence $\alpha - 1$ is an even number and the $\alpha - 1$ subgroups $H_1, H_{s_2}, \ldots, H_{s_{\alpha-1}}$ could only be transformed according to a group T' having two transitive constituents. But by Theor. 8 this is impossible. Hence the theorem.

§6.—*Certain Primitive Groups of Odd Order contained in the Holomorph of the Abelian Group P of Order p^m (p an odd prime) of Type* $(1, 1, \ldots, 1)$.

Represent P as a regular group. Suppose that the order of its group of isomorphisms L is divisible by q^n (q an odd prime). To any subgroup of order q^n in L there corresponds in the holomorph of P a transitive group of degree p^m, and of order $p^m q^n$. The subgroup of this transitive group, which leaves a given letter fixed, is of order q^n, and is clearly maximal, if m is the index to which p belongs mod q. Hence,

THEOREM 12.—*If $p^m \equiv 1 \bmod q^n$ ($n \not< 1$), m being the index to which p belongs mod q, there is a primitive group G of order $p^m q^n$ contained in the holomorph of the abelian group of order p^m of type* $(1, 1, \ldots, 1)$.

Cor. 1. *If q^n is the highest power of q which divides $p^m - 1$, there is only one group G satisfying the above conditions.*

Cor. 2. *If $p-1$ ($p \neq 3$) is not divisible by 3, there exists a primitive group G of degree p^2 and of order $3p^2$. Furthermore, if $p-1$ is divisible by 3, there is no primitive group of degree p^2 whose order is $3p^2$.*

The first part of this corollary is merely a special case of the general theorem.

The second part may be proved as follows:

By Sylow's theorem, a group of this order contains a single subgroup P of

order p^2. Since G is primitive, an invariant subgroup P must be transitive. The subgroup is, therefore, regular, and it must be the non-cyclical group of order p^2. P would contain $p+1$ subgroups of order p, these would have to occur in conjugate sets of three, since G cannot contain an invariant intransitive subgroup. But $p+1$ is not divisible by 3 when $p-1$ is divisible by 3.

§7.—*On the Class of Primitive Groups G of Odd Order.*

By the class of a substitution group is meant the smallest number of elements in any one of its substitutions besides identity.*

Let $n-\mu$ represent the class of G. For all odd values of μ less than 7 there exist groups G of odd order of class $n-\mu$. Thus:

For $\mu=1$, in any non-cyclic invariant subgroup of a metacyclic group.
For $\mu=3$, in the primitive group of degree 27 of order 27.39.†
For $\mu=5$, in the primitive group of degree 125 of order 125.93.‡

It will now be shown that there is no primitive group of odd order in which μ is even and less than 6. G_s has an even number of transitive constituents in pairs of the same degree (p. 10), and is clearly formed by establishing a simple isomorphism between its transitive constituents. If $\mu=2$, at least two of the transitive constituents must be non-regular, since they are in pairs of the same degree. Suppose that t_1 is the degree of one of these non-regular transitive constituents. It must clearly be of class t_1-1. In the constituent of degree $2t_1$ formed by combining these two, every substitution of degree t_1-1 would correspond to a substitution of degree t_1, or G would contain substitutions of degree $n-3$. But this is clearly impossible, since a transitive group of degree t_1 and of class t_1-1, the order of the substitutions of degree t_1 is prime to the order of those of degree t_1-1.

It remains to consider the case when $\mu=4$. Here again G_s must be formed by establishing a simple isomorphism between transitive constituents, not all of which can be regular. If t_1 is the degree of any non-regular transitive constituent, this constituent must either be of class t_1-3 or t_1-1. Suppose that all

* Jordan, Liouville, Vol. 16 (1871), p. 408.
† Burnside, loc. cit., p. 180.
‡ See p. 30 of this paper.

the non-regular transitive constituents are of class one less than their degrees. Since there must be an even number of such transitive constituents, it readily follows that G_s cannot have more than two such transitive constituents or G would contain substitutions of degree less than $n-4$. But in this case G would have no substitutions of degree less than $n-3$. Hence G_s must have at least one transitive constituent T of some degree t_2 of class t_2-3. Now, G_s must have at least one more transitive constituent T' of degree t_2. This constituent must be of class t_2-1 or t_3-1. In combining T and T' into a constituent of degree $2t_2$, all the substitutions of degree t_2-3 in one must correspond to substitutions of degree t_2 in the other or G would contain substitutions of degree less than $n-4$. From this it is easily seen that substitutions of degree t_2-3 and those of degree t_2 to which they correspond must be regular. Hence all the substitutions of degree t_2-3 would be of order 3. Consider the subgroup P_3 of G_s corresponding to a subgroup of T of degree t_2-3 of order 3^α such that there is no subgroup of T of order $3^{\alpha+1}$ which is of degree t_2-3. P_3 would then be invariant in a subgroup of G of degree n, and the 4 letters of G not occurring in P_3 would be transitively connected so that the order of G must be an even number. Hence there is no primitive group of odd order of class $n-4$.

PART II.

§8.—*On the Primitive Groups of Odd Order of Degree less than* 243.

It is known* that all transitive groups of odd order of prime degree are invariant subgroups of the metacyclic group. Inasmuch as these groups are well known, we shall consider only those primitive groups whose degrees are not primes. As already stated in this paper (p. 1), the primitive groups of odd order have been determined for degrees not exceeding 100. It is the object of this part to extend this determination to all degrees less than 243. We are then concerned with the groups whose degrees lie between 100 and 243. It is stated without proof by Burnside (loc. cit., note, p. 185) that any transitive group of odd order of degree $3p$ (p a prime) is imprimitive. We have examined all the com-

* Burnside, loc. cit., p. 177.

posite numbers within the given limits for the degrees of primitive groups of odd order, and the results agree with this statement. We shall, therefore, for the sake of brevity, omit these degrees.

Represent by G^n a primitive group of odd composite order of degree n. As in Part I, let G_s denote the subgroup of G^n containing all the substitutions which leave a given letter a_s fixed. The method is, briefly, as follows:

For each odd degree n (n not a prime nor 3 times a prime) it is assumed that a group G^n exists. The degree of any solvable primitive group is a power of a prime.* Hence, in order to prove that no group G^n exists, for a given value of n which is not the power of a prime, it is sufficient to prove that there is no simple group G^n, provided there is no simple group of odd composite order of degree less than n. As the latter condition is satisfied, it is further assumed that G^n is simple when it is not a power of a prime.

We write down for examination all those, and only those, systems of intransitivity of G_s which are not excluded by the conditions, 1°, that every prime which divides the order of one transitive constituent divides the order of every transitive constituent;† 2°, that the transitive constituents occur in pairs of the same degree;‡ 3°, that when G^n is simple, there can be no transitive constituent whose degree is a prime of the form $2^m + 1$;§ 4°, that if the degree of one transitive constituent is a prime of the form $2^m + 1$, all the transitive constituents are of this degree.

This method of excluding transitive constituents of G_s depends, of course, on a knowledge of the primes which occur in the orders of transitive groups of odd order of degree less than $n/2$. The following table shows the primes which may occur in the orders of transitive groups of odd order of degree less than 120. The primes written under the degree are the primes which occur in the orders of some transitive groups of odd order of the given degree in addition to those primes contained in the degree itself.

---

* Lettre de Galois, a M. Auguste Chevalier, Liouville's Journ. (1846), p. 41.

† Jordan, loc. cit., p. 284. ‡ Burnside, loc. cit., p. 165. § Miller, loc. cit., p. 6.

Degree:	3	5	7	9	11	13	15	17	19	21	23
Primes:			3		5	3			3		11
Degree:	25	27	29	31	33	35	37	39	41	43	45
Primes:	3	13	7	3, 5	5	3	3		5	3, 7	
Degree:	47	49	51	53	55	57	59	61	63	65	67
Primes:	23	3		13			29	3, 5		3	3, 11
Degree:	69	71	73	75	77	79	81	83	85	87	89
Primes:	11	5, 7	3		3, 5	3, 13	5, 13	41		7	11
Degree:	91	93	95	97	99	101	103	105	107	109	111
Primes:	3	5	3	3	5	5	3, 17		53	3	
Degree:	113	115	117	119							
Primes:	7	11		3.							

We shall use $S_1, S_2, \ldots, S_t$ to represent the sets of systems of intransitivity of G_s which are not excluded by the conditions above stated. The transitive constituents thus obtained are either shown to lead to impossibilities or the orders and number of the groups are determined.

§9.—*Determination of the Groups* G^n $(100 < n < 243)$.

G^{105}.

$S_1 = 13, 13, 13, \ldots, 13.$ $\qquad$ $S_2 = 13, 13, 39, 39.$

If G_s has systems S_1, the order of G^{105} would, by Cor. 2, Theor. 3, be $5 \cdot 13 \cdot 3^{\alpha} \cdot 7$ $(\alpha \geqslant 2)$. But G^{105} would then contain in its order less than 7 prime factors, and could not be a simple group.* If G_s has systems S_2, the order of G would be $5 \cdot 13 \cdot 7 \cdot 3^{\beta}$ (Cor. 1, Theor. 3). Let $p = 5$ in Cor. 2, Theor. 1, and it follows that G^{105} does not exist.

G^{115}.

$S_1 = 19, 19, \ldots, 19.$ $\qquad$ $S_2 = 57, 57.$

G^{115} would be of order $3^{\alpha} \cdot 5 \cdot 19^{\beta} \cdot 23$. Let $p = 23$ in Cor. 2, Theor. 1, and it follows that G^{115} does not exist.

---

* Burnside, loc. cit., pp. 265–268.

G^{117}.

$$S_1 = 29, 29, 29, 29.$$

The order of G_s would be, by Cor. 2, Theor. 3, $29 \cdot 7^\alpha$ $(\alpha \geqslant 1)$. But G^{117} would then contain in its order less than 7 primes, and could therefore not be a simple group.

G^{119}.

$$S_1 = 59, 59.$$

G^{119} would be of order $17 \cdot 7 \cdot 59^\alpha \cdot 29^\beta$. Let $p = 17$ in Cor. 2, §1, and it follows that G^{119} does not exist.

G^{121}.

$S_1 = 3, 3, \ldots, 3.$ $\quad$ $S_3 = 15, 15, \ldots, 15.$

$S_2 = 5, 5, \ldots, 5.$ $\quad$ $S_4 = 15, 15, 45, 45.$

If G_s has systems S_1 the order of G^{121} would be $121 \cdot 3$.* By Cor. 2, §6, there is a group of order $3 \cdot 121$, and it is easily seen that there is only one such group. With S_2, the order of G^{121} would be $121 \cdot 5$. Any group of this order contains at least one invariant subgroup of order 11. As this subgroup would be intransitive, it cannot occur in a primitive group.

If G_s has systems S_3 or S_4, the order of G^{121} would be of the form $11^2 \cdot 3^\alpha \cdot 5^\beta$ If any transitive constituent of degree 15 has 5 systems of imprimitivity the order of G_s is not divisible by 5^2 (Theor. 4). G^{121} would then be of order $11^2 \cdot 3^\alpha \cdot 5$. The subgroup of order 3^α would then be of degree 120. If $\alpha > 1$, from §3, G^{121} would contain an intransitive subgroup having a transitive constituent of degree $1 + 3k$ $(k > 1)$, and whose order is divisible by 3. The number of the form $1 + 3k$ could only be 55 and be a divisor of the order. But no transitive group of degree 55 of odd order has its order divisible by 3. The transitive constituents of degree 15 must then all have 3 systems of imprimitivity, and G^{121} would be of order $121 \cdot 3 \cdot 5^\beta$. If $\beta > 1$, it follows from §3 that a subgroup P of greatest order common to two subgroups of G^{121}, leaving given letters fixed, is invariant in a subgroup of order $11^2 \cdot 5^\beta$, $11 \cdot 3 \cdot 5^\beta$ or $11 \cdot 5^\beta$. The conjugate set to which

* Miller, loc. cit., p. 536.

P belongs under G^{121} would then be transformed by G^{121}, according to a transitive group of degree 3, 11 or 33. Now, it is easily seen that $\beta \not> 2$. We shall show that one group G^{121} exists when $\beta = 1$, and none when $\beta = 2$.

A group of order $11^2 . 5^\beta . 3$ ($\beta \not> 2$) must, by Sylow's theorem, contain an invariant subgroup P_{121} of order 11^2. This subgroup in G^{121} must be of type (1, 1), since the cyclical group would contain a single subgroup of order 11 which would be an invariant intransitive subgroup of G^{121}. The group G^{121} must then occur in the holomorph of P_{121}. The group of isomorphisms L of P_{121} is of order $120 . 110 = 3 . 5^2 . 2^4 . 11$. Now, L contains just 55 subgroups* of order 3, each being invariant in a subgroup of order $3 . 5 . 2^4$. Hence L contains subgroups of order 15 and they are all conjugate. It results, therefore, that the transitive groups of order $121 . 15$ in the holomorph of G_{121} are conjugate. The subgroup of order 15 which leaves a giving letter fixed, is clearly maximal. Hence the group is primitive. Similarly, examining L, it is found to contain no subgroups of order $3 . 5^2$. Hence there is no group G^{121} of order $11^2 . 3 . 5^2$ contained in the holomorph of P^{121}.

$$G^{125}.$$

$$S_1 = 31, 31, 31, 31.$$

The order of G^{125} would be $5^\alpha . 31 . 3^\beta$ ($\alpha = 3$ or 4, $\beta = 0$ or 1, Cor. 2, §2). By Sylow's theorem, G^{125} would contain 1 or 31 subgroups of order 5^α. If it contained only one, $\alpha = 3$; for, if $\alpha = 4$, G_s and its conjugates would contain more than 5^4 substitutions of order 5. If it contained 31 subgroups of order 5^α, they would be transformed by G^{125} according to a non-cyclic transitive group of degree 31 isomorphic with G^{125}. The subgroup of G^{125} corresponding to identity on this quotient group would contain a single subgroup of order 5^3. Any group G^{125} then contains an invariant subgroup P_{125} of order 125. The group P_{125} must be the abelian group of type (1, 1, 1), since all other groups of order 125 contain characteristic subgroups, and a characteristic subgroup of P_{125} would be an invariant intransitive subgroup of G^{125}. The group G^{125} is then contained in the holomorph of P_{125}. The group of isomorphisms L of P_{125} is of order $2^7 . 3 . 5^3 . 31$. The group L contains, by Sylow's theorem, 1, 2^5, 5^3 or $2^5 . 5^3$ subgroups of order

* This is shown from the composition series of L. The factor groups of L are the cyclic group of order 10, the simple group of order 660 representable on 11 letters, and the group of order 2.

31. That it could not contain 1 or 2^5 such subgroups is easily seen from tne fact that L occurs as a transitive group of degree 124. In L a subgroup of order 31 is then invariant in a subgroup of order $31 \cdot 2^2 \cdot 3$ or $31 \cdot 2^7 \cdot 3$. Hence L contains subgroups of order 31 and $31 \cdot 3$, but it does not contain any subgroup of order $31 \cdot 5$ or $31 \cdot 15$. Corresponding to these subgroups, there are in the holomorph of P_{125} transitive groups of orders $5^3 \cdot 31$ and $5^3 \cdot 31 \cdot 3$. These groups are evidently primitive groups. That there is only one group G^{125} of each of these orders follows from the fact that in L the subgroups of each of the orders 31 and $31 \cdot 3$ form a single conjugate set.

G^{133}.

$S_1 = 11, 11, \ldots, 11.$ $\quad$ $S_4 = 27, 27, 39, 39.$

$S_2 = 11, 11, 55, 55.$ $\quad$ $S_5 = 27, 27, 13, 13, \ldots, 13.$

$S_3 = 33, 33, 33, 33.$

If G_s has systems S_1 or S_2, the order of G^{133} would be of the form $19 \cdot 7 \cdot 11^\alpha \cdot 5^\beta$. Let $p = 19$ in Cor. 2, §1, and it follows at once that G^{133} does no exist in the case under consideration.

If G_s has systems S_3, the order of G^{133} would be $19 \cdot 7 \cdot 11^\alpha \cdot 5^\beta \cdot 3^\gamma$. From §3 it follows that $\alpha = 1$. Now, it is easily seen that an imprimitive group of odd order of degree 33 whose order is not divisible by 11^2, does not have its order divisible by 5^2. Hence, the order of any transitive constituent T would be $11 \cdot 3^{\alpha_1} \cdot 5^{\beta_1}$. $(\beta_1 \geqslant 1)$. Corresponding to identity in T, there could be no substitutions of order 5 or there would also be substitution of order 11, and the order of G_s would be divisible by 11^2. Hence, $\beta \geqslant 1$. If $\beta = 1$, G^{133} contains an invariant subgroup of index 5.* If $\beta = 0$, G^{133} contains an invariant subgroup of index 11. Hence, G^{133} does not exist if G_s has systems S_3.

If G_s has systems S_4 or S_5, the order of G^{133} is of the form $7 \cdot 19 \cdot 3^\alpha \cdot 13^\beta$. The transitive constituents of degree 27 must be primitive groups. Let T_1 and T_2 represent the transitive constituents of degree 27. Consider the invariant subgroup H_s of G_s corresponding to identity in T_1. If any elements of T_2 occur in H_s, the latter must have a transitive constituent of degree 27, which is an invariant subgroup of T_2. Now, it is easily seen that an imprimitive group of degree 39 of odd order cannot contain a transitive subgroup of degree 27. Hence a conjugate G_r of G_s in which H_s occurs would contain a transitive constituent of

* Burnside, loc. cit., pp. 261–262.

degree 27 having the same elements as T_2. $\{G_r, G_s\}$ would then be an intransitive group. But $\{G_r, G_s\}$ must coincide with G^{133}, since G_s is maximal. Hence H_s has no transitive constituent of degree 27.

T_1 and T_2 must then be combined by establishing a simple isomorphism between them, and H_s could only be of degree $\leqq 39 . 2$. From the fact that $2 . 27$ of the conjugates of H_s under G^{133} contained in G_s would be transformed according to the constituent of degree 54 in G_s, this assumption as to the degree of H^s readily leads to impossibilities. Hence, the order of G_s is equal to the order of its transitive constituent of degree 27. The order of G^{133} would then be $133 . 3^\alpha . 13$ ($\alpha \geqslant 4$), but a group of this order could not, by Sylow's theorem, contain more than 39 subgroups of order 19. Hence G^{133} does not exist.

G^{135}.

$S_1 = 67, 67.$ $\qquad$ $S_2 = 27, 27, 27, 27, 13, 13.$

If G_s has systems S_1, the order of G^{135} would be $67 . 5 . 3^\alpha . 11^\beta$ ($\alpha \geqslant 4$, $\beta = 0$ or 1, Cor. 2, Theor. 3). Let $p = 5$ in Cor. 2, Theor. 1, and it follows that G^{135} does not exist. If G_s has systems S_2, the order of G^{135} is $5 . 3^\alpha . 13$. By Sylow's theorem, a group of this order contains not more than 13 subgroups of order 3^α, Hence G^{135} does not exist.

G^{143}.

$S_1 = 71, 71.$

G^{143} would be of order $11 . 13 . 71 . 5^\alpha . 7^\beta$ ($\alpha \leqq 1$, $\beta \leqq 1$) Cor. 2, Theor. 3. As this order would be the product of distinct primes, G^{143} cannot be a simple group* and therefore does not exist.

G^{145}.

$S_1 = 9, 9, \ldots, 9.$ $\qquad$ $S_2 = 9, 9, \ldots, 9, 27, 27.$

$S_3 = 9, 9, \ldots, 9, 27, 27, 27, 27.$

The group G^{145} would be of order $29 . 5 . 3^\alpha$. Let $p = 29$ in Cor. 2, Theor. 1 and it follows that G^{145} does not exist.

---

* Frobenius, Berliner Sitzungsberichte (1893), p. 337.

G^{147}.

$S_1 = 73, 73.$

By Cor. 2, Theor. 3, the order of G^{147} would be $7^2 . 73 . 3^\alpha$ ($\alpha \geqslant 3$). But a group of this order would, by Sylow's theorem, contain a single subgroup of order 7^2. As this subgroup would be an invariant intransitive subgroup, no group G^{147} exists.

G^{153}.

$S_1 = 19, 19, \ldots, 19.$ $\qquad$ $S_2 = 19, 19, 57, 57.$

The group G^{153} would be of order $17 . 3^\alpha . 19^\beta$. If in Cor. 2, §1, we make $p = 17$, it follows that G^{153} does not exist.

G^{155}.

$S_1 = 11, 11, \ldots, 11.$ $\qquad$ $S_2 = 11, 11, 11, 11, 55, 55.$ $\qquad$ $S_3 = 77, 77.$

$S_4 =$ any set of systems in which one system contains 7 letters. If G_s has systems S_1 or S_2, its order is not divisible by 11^2 (§2, Cor.) The order of G^{155} would then be $11 . 31 . 5^\alpha$. By Sylow's theorem, a group of this order would contain 1, 11, 31 or 341 subgroups of order 5. It could not contain 1, 11, 31 and be a simple group, since there is no simple group of odd composite order of degree < 155. If G^{155} contains 341 subgroups of order 5^α, it occurs as a primitive group of degree 341. Since 340 is not divisible by 5^2, the order of the subgroup which leaves a given letter fixed would not exceed 5. But a group of order $31 . 11 . 5$ is clearly solvable. If G_s has systems S_3, the order of G^{155} is of the form $31 . 5^\alpha . 7^\beta . 11^\gamma . 3^\delta$. Let $p = 11$ and 7 in Cor., §3, and it follows that $\gamma = 1$ and $\beta = 1$. Since G_s has only two transitive constituents, it follows that the order of G_s is equal to that of one of its transitive constituents. But if the order of a transitive group of odd order of degree 77 is not divisible by 11^2 nor 7^2, its order is not divisible by 5^2 nor 3^2. Hence $\alpha \leqq 2$ and $\delta \leqq 1$.

If G_s has systems S_4, the order of G^{155} is of the form $5 . 31 . 7^\alpha . 3^\delta$ and G^{155} contains an invariant subgroup of index 5. If G^{155} exists, its order would then be of the form $3^{\alpha_1} . 5^{\alpha_2} . 7 . 11 . 31$ ($\alpha_1 = 0$ or 1, $\alpha_2 \geqslant 2$), but a group of this order cannot be a simple group as this number contains less than 7 prime factors. Hence G^{155} does not exist.

G^{161}.

$S_1 = 15, 15, 15, 15, 25, 25, \ldots, 25.$ $S_2 = 27, 27, 27, 27, 13, \ldots, 13.$

The order of G^{161} would be of the form $7.23.5^{\alpha}.5^{\beta}.13^{\gamma}$. Let $p = 23$ in Cor. 2, Theor. 1, and it follows that G^{161} does not exist.

G^{165}.

$S_1 = 41, 41, 41, 41.$

By Cor. 2, Theor. 3, the order of G^{165} would be $11.5^{\alpha}.3.41$ ($\alpha \geqslant 2$), and G^{165} would, by Sylow's theorem, contain a single subgroup of order 11. Hence G^{165} does not exist.

G^{169}.

$S_1 = 3, 3, \ldots, 3.$
$S_2 = 7, 7, \ldots, 7.$
$S_3 = 7, 7, \ldots, 7, 21, 21.$
$S_4 = 7, 7, \ldots, 7, 21, 21, 21, 21.$
$S_5 = 7, 7, \ldots, 7, 21, 21, 21, 21, 21, 21.$
$S_6 = 21, 21, \ldots, 21.$
$S_7 = 21, 21, 63, 63.$
$S_8 = 7, 7, \ldots, 7, 49, 49.$
$S_9 = 7, 7, 7, 7, 21, 21, 49, 49.$
$S_{10} = 7, 7, \ldots, 7, 63, 63.$

If G_s has systems S_1, the order of G^{169} is $13^2.3$, but by Cor. 2, §6, there is no group G^{169} of this order.

If G_s has some transitive constituent of degree 7, the order of G^{169} is of the form $13^2.7.3^{\alpha}$ (Cor. 2, Theor. 3). G^{169} would contain 13, 91 or 169 subgroups of order 3^{α}, if $\alpha > 0$. For, since the number of such subgroup in G_s must be 7, the total number in G^{169} is $\frac{7.169}{\lambda}$, where λ is the number of letters of G^{169} left fixed by a subgroup of order 3^{α}, and $\lambda > 1$.

If the number is 13 or 91, by considering the isomorphic group of degree 13 or 91, according to which the conjugate set is transformed, it is easily seen that $\alpha \geqslant 3$. If the number is 169, a subgroup of order 3^{α} is invariant in a subgroup K of order $3^{\alpha}.7$ and of degree 169, since in any subgroup leaving a given letter fixed, a subgroup of order 3^{α} is one of 7 conjugates. Since a substitution of order 7 in G^{169} is of degree 168, every transitive constituent of K has its order divisible by 7. Now there is no transitive group of odd order of degree 3^{β} when $3^{\beta} < 169$, which contains in its order the factor 7. Hence the degree of every transitive constituent of K is a multiple of 7. But 7 is not a divisor of 169.

Hence there cannot be 169 subgroups of order 3^α. We have then shown that α is not greater than 3 when G_s has a transitive constituent of degree 7.

In all the remaining cases G^{169} would be of order $13^2.7^\alpha.3^\beta$. Let $p = 7$ in Cor., §3, and it follows that $\alpha = 1$. If T is a subgroup such that there is no subgroup of greater order common to two subgroups of order 3^β, then T is of order $3^{\beta-1}$. From the reasoning of §3, it follows that T is invariant in a subgroup of degree 169 of one of the following orders: $13^2.3^\beta$, $13.7.3^\beta$, 13.3^β or 7.3^β. The subgroup T would then be one of 7, 13, 91, or 169 conjugates in G^{169} and just as before it follows that $\beta \not> 3$.

It remains to consider the group G^{169} of order $13^2.7.3^\beta$ ($\beta \not> 3$). By Sylow's theorem a group of this order contains 1 or 27 subgroups of order 13^2. It could not contain 27; for, on account of the limitations on β, they would be transformed according to a regular group of degree 27. Hence G^{169} contains a single subgroup order 13^2, and is contained in the holomorph of the abelian group P of order 13^2 of type (1, 1). The group of isomorphisms L of P is of order $2^5.3^2.7.13$. It remains to examine L for subgroups of order 7.3^β ($\beta \not> 3$). Such a subgroup contains a single subgroup of order 7. The group L contains just 78 subgroups of order 7.* Each of these is then invariant in a subgroup of order $7.3.2^4$. From this† it follows that L contains subgroups of order 7 and 21 but none of order 7.3^β ($\beta > 1$). The subgroups of order 21 are conjugate in L. Hence there is in the holomorph of P just one subgroup of each of the orders 169.7 and 169.21. The subgroup leaving a given letter fixed is in each case maximal. Hence the groups are primitive.

G^{171}.

$S_1 = 15, 15, \ldots, 15, 25, 25.$ $\quad S_2 = 15, 15, 45, 45, 25, 25.$ $\quad S_3 = 85, 85.$

If G_s has systems S_1 or S_2, by Theor. 4, the order of G_s cannot be divisible by 3^2, since the order must be divisible by 5^2 on account of the transitive constituent of degree 5^2. The order of G^{171} is then of the form $19.3^3.5^\alpha$. Let $p = 5$ in Cor., §3, and it follows that $\alpha = 1$. As a group of $19.3^3.5$ contains a single subgroup of order 19, there is no simple group G in which G_s has systems S_1 or S_2.

* Shown by considering the composition series of L. The factor groups of L are the cyclical group of order 12, the simple group of order 1092, and the group of order 2. † Ibid.

If G_s has systems S_3, by Theor. 4, the order of G^{171} would be $19.3^2.5.17^\alpha$ or $19.3^2.17.5^\beta$. But groups of these orders cannot be simple.* Hence G^{171} does not exist.

G^{175}.

$S_1 = 29, 29, \ldots, 29.$ $\qquad$ $S_2 = 87, 87.$

If G_s has systems S_1, by Cor. 2, Theor. 3, the order of G^{175} would be $7^\alpha.5^2.29$ $(\alpha \geqslant 2)$. But a group of this order cannot be a simple group, since it contains not more than 5 prime factors. If G_s has systems S_2, the order of G^{175} is $7^\alpha.5^2.29^\beta.3^\gamma$. Let $p = 29$ in Cor., §3, and it follows that $\beta = 1$. Since G_s has only two transitive constituents, its order is equal to the order of each of its constituents (Theor. 10). Making use of this fact, it is easily seen that 7 cannot occur to a higher power in the order of G_s than the power to which 29 occurs. Hence $\alpha \geqslant \beta + 1$. If either transitive constituent of G_s has 3 systems of imprimitivity, the order of G_s^{175} is not divisible by 3^2. But the order of G^{175} would then contain not more than 6 prime factors. Hence each transitive constituent must have 29 systems of imprimitivity. G_s would then contain an invariant subgroup of order 3^γ. Now the subgroup of such an imprimitive group which leaves a given letter fixed would leave 3 letters fixed. The subgroup K, containing all the substitutions common to G_s and any one of its conjugates G_r, is of order $7^{\alpha-1}\,3^{\gamma-1}$ and is invariant in subgroups of G_s and G_r whose orders are equal to $7^{\alpha-1}.3^\gamma$ and which contain a single subgroup of order 3^γ. The subgroup of G^{175} which contains all the substitutions which transform K into itself contains $1 + 3k\,(k > 0)$ subgroups of order 3^γ. Its order could then only be $7^\alpha.3^\gamma$ or $7^{\alpha-1}\,5^2.3^\gamma$ (other assumptions lead to transitive representations of G^{175} of degree less than 175). If subgroups of these orders occur in G^{175}, it can be represented as a transitive group of degree 725 or 203. Since any divisor of these numbers is less than 175, these representations would be primitive. As a group of degree 725 the subgroup which leaves a given letter fixed would be of order $7^\alpha.3^\gamma$. As it is easily shown that there is no transitive group of odd order of degree $3^\delta\,(\delta < 6)$ whose order contains the factor 7, the degree of each transitive constituent of above subgroup would be a multiple of 7. But 7 is not a divisor of 724. As a group of degree 203, the subgroup which leaves a given letter fixed would be of

* Burnside, loc. cit., p. 262.

order $7^{\alpha-1}.5^2.3^\gamma$. But no intransitive group of degree 202 of this order can be constructed in which every prime which divides the order of one transitive constituent divides the order of every transitive constituent, and in which the transitive constituents are in pairs of the same degree.

G^{185}.

$S_1 = 23, 23, \ldots, 23.$ $S_2 = 27, 27, 13, 13, \ldots, 13.$

$S_3 = 27, 27, 39, 39, 13, 13, \ldots, 13.$

The order of G^{185} would be of the form $5.37.23^\alpha.11^\beta.3^\gamma.13^\delta$. But a group of this order cannot be simple.*

G^{187}.

$S_1 = 31, 31, 31, \ldots, 31.$ $S_3 = 93, 93.$

$S_2 = 27, 27, 27, 27, 13, 13, \ldots, 13.$ $S_4 = 27, 27, \ldots, 27, 39, 39.$

The order of G^{187} is of the form $17.11.3^\alpha.31^\beta.13^\gamma$. Let $p = 17$ in Cor. 2, §1, and it follows that G^{187} does not exist.

G^{189}.

$S_1 = 47, 47, 47, 47.$ $S_2 = 13, 13, 27, 27, \ldots, 27.$

$S_3 = 13, 13, 81, 81.$

If G_s has systems S_1. the order of G^{189} is of the form $7.3^3.47.23^\alpha$ ($\alpha = 0$ or 1). As the order contains at most 6 prime factors, the group cannot be simple. If G_s has systems S_2 or S_3, the order of G^{189} is $7.13.3^\alpha$ (Cor. 2, §2). By Sylow's theorem, a group of this order contains not more than 91 subgroups of order 3. The group G^{189} could then occur on as few as 91 letters, but this has been shown impossible. Hence G^{189} does not exist.

G^{195}.

$S_1 = 97, 97.$

The group G^{195} would be of order $5.13.3^\alpha.97$ (Cor. 2, Theor. 3). Let $p = 5$ in Cor. 2, §1, and it follows that G^{195} does not exist.

---

* Burnside, loc. cit., p. 170.

G^{203}.

$S_1 = 101, 101.$

By Cor. 2, Theor. 3, the order of G^{203} would be $7.29.101.5^{\alpha}$ ($\alpha \geqslant 2$). As this number contains not more than 5 prime factors, the group cannot be simple. Hence G^{203} does not exist.

G^{205}.

$S_1 = 51, 51, 51, 51.$

The order of G^{205} would be of the form $5.41.3^{\alpha}.17^{\beta}$. Let $p = 5$ in Cor. 2, §1, and it follows that G^{205} does not exist.

G^{207}.

$S_1 = 103, 103.$

The order of G^{207} would be of the form $23.3^{\alpha}.103.17$ (Cor. 2, Theor. 3). Let $p = 23$ in Cor. 2, §1, and it follows that G^{207} does not exist.

G^{209}.

$S_1 = 13, 13, \ldots, 13.$ $\quad S_2 = 13, 13, \ldots, 13, 39, 39.$

$S_3 = 13, 13, 13, 13, 39, 39, 39, 39.$

If G_s has systems S_1 or S_2, it is easily seen that the order of G^{209} is equal to or a divisor of $11.19.13.3$; but a group of this order cannot be simple, as the order is the product of distinct primes. If G_s has systems S_3, the order of G^{209} is $11.19.13^{\alpha}.3^{\beta}$. Let $p = 11$ in Cor. 2, §1, and it follows that G^{209} does not exist.

G^{215}.

$S_1 = 107, 107.$ $\quad S_2 = 13, 13, 13, 13, 27, 27, \ldots 27.$

$S_3 = 13, 13, \ldots, 13, 81, 81.$

The order of G^{215} would be of the form $5.43.107^{\alpha}.53^{\beta}.13^{\gamma}.3^{\delta}$. But a group of this order cannot be simple.* Hence G^{215} does not exist.

* Burnside, loc. cit., p. 170.

G^{217}.

$S_1 = 9, 9, \ldots, 9.$
$S_2 = 9, 9, \ldots, 9, 27, 27.$
$S_3 = 9, 9, \ldots, 9, 81, 81.$
$S_4 = 9, 9, \ldots, 9, 27, 27, 27, 27.$
$S_5 = 27, 27, 27, 27, 27, 27, 9, 9, \ldots, 9$
$S_6 = 27, 27, \ldots, 27.$
$S_7 = 27, 27, 81, 81.$

For all these systems, except when in S_6 and S_7, the transitive constituents of degree 27 are primitive groups, the order of G_s is a power of 3. The order of G^{217} would then be $31.7.3^\alpha$, with the exception just mentioned. From the argument of §3, it readily follows that, if $\alpha > 3$, G^{217} would contain a subgroup of order $\geqq 3^{\alpha-2}.7$, which order contains a factor $\equiv 1 \bmod 3$. If the order of the subgroup were greater than this number, such a subgroup would lead to a transitive representation of the simple group on less than 217 letters. Hence the subgroup, if G^{217} exists, is of order $3^{\alpha-2}.7$. The simple group would then occur as a transitive group of degree $\frac{31.7.3^\alpha}{7.3^{\alpha-2}} = 279$. When represented on 279 letters the group would be primitive and the subgroup which leaves a given letter fixed would be of order $7.3^{\alpha-2}$. The degrees of all transitive constituents would be multiples of 7. But 7 is not a divisor of 278.

It remains to consider the case where G_s has for some of its transitive constituents primitive groups of degree 27. In this case all the transitive constituents are either primitive groups of degree 27 or two of them are imprimitive groups of degree 81. In the former case, by Cor., Theor. 6, §4, the order of G^{217} would be $7.31.3^\alpha.13$ ($\alpha \geqq 4$). But, by Sylow's theorem, a group of this order contains no more than 63 subgroups of order 31. But this is impossible, since the simple group of odd order would occur of degree 63. In the latter case, we shall also show that the order G_s cannot exceed that of one of the transitive constituents of degree 27. Let T' be the transitive constituent of degree 27 distinct from T. Let H_s be the invariant subgroup of G_s corresponding to identity in T, where T is so selected that its order is not greater than that of T'. Then, by Theor. 9, 27 of the subgroups $H_{s_1}, H_{s_2}, \ldots, H_{s_{\alpha-1}}$ (defined in §2) are transformed by G_s according to T'. These 27 subgroups can contain no elements contained in T', or H_s would have some transitive constituents of degree 13, which is impossible. Hence, these 27 subgroups generate a subgroup contained in the invariant subgroup of G_s corresponding to identity in T'. But this is impos-

sible, since, by hypothesis, the order of T' is equal to or greater than the order of T.

G^{221}.

$S_1 = 11, 11, \ldots, 11.$ $S_4 = 15, 15, \ldots, 15, 25, 25, 25, 25.$
$S_2 = 11, 11, \ldots, 11, 55, 55.$ $S_5 = 15, 15, 25, 25, 25, 25, 45, 45.$
$S_3 = 55, 55, 55, 55.$

If G_s has systems S_1, the order of G^{221} is, by Cor. 2, Theor. 3, $17.13.11.5^\alpha$ $(\alpha \geqslant 1)$. But a group of this order cannot be simple, since it is the product of distinct primes.* If G_s has any of the other systems, the order of G^{221} is $17.13.5^\alpha.3^\beta.11^\gamma$. Let $p = 17$ in Cor. 2, §1, and it follows that G^{221} does not exist.

G^{225}.

$S_1 =$ any set of systems in which some systems contain 7 letters.
$S_2 = 21, 21, \ldots, 21, 49, 49.$ $S_3 = 63, 63, 49, 49.$

If G_s has some transitive constituents of degree 7, the order of G^{225} is of the form $5^2.3^\alpha.7$ (Cor. 2, Theor. 3). But, by Sylow's theorem, a group of this order cannot contain more than 175 subgroups of order 3^α. If G_s has systems S_2 or S_3, the order of G^{225} is of the form $5^2.3^\alpha.7^\beta$. Let $p = 7$ in Cor., §3, and it follows that $\beta = 1$. Then as above G^{225} would contain no more than 175 subgroups of order 3^α. Since there is no simple group of odd composite order of degree 175 the group G^{225} does not exist.

G^{231}.

$S_1 = 15, 15, 25, 25, \ldots, 25.$ $S_5 = 45, 45, 45, 45, 25, 25.$
$S_2 = 15, 15, 25, 25, 75, 75.$ $S_6 = 23, 23, \ldots, 23.$
$S_3 = 15, 15, \ldots, 15, 25, 25.$ $S_7 = 115, 115.$
$S_4 = 15, 15, \ldots, 15, 25, 25, 45, 45.$

If G_s has some transitive constituent of degree 15, the order of G_s is not divisible by 3^2 (Theor. 4). Then G^{231} would be of order $3^2.7.11.5^\alpha$ and would contain an invariant subgroup of index 3^2.† If G_s has systems S_6 or S_7, the

* Frobenius, loc. cit., p. 337.

† Burnside, loc. cit., pp. 260, 262.

order of G^{231} would be of the form $3.7.11^{\alpha}.23^{\beta}.5^{\gamma}$; but a group of this order has an invariant subgroup of index 3.

If G_s has systems S_5, the constituents of degree 25 are the primitive group of order 75. As this group is of class 24, we have, by Cor. 3, Theor. 3, that the order of G_s is not divisible by 5^3. The group G^{231} would then be of order $3^{\alpha}.5^2.7.11$. By Sylow's theorem, a group of this order which does not contain less than 231 subgroups of order 3^{α}, contains 385 such subgroups. A simple group of this order would then occur as a primitive group of degree 385. The subgroup G_1, leaving a given letter fixed, would then be of order 5.3^{α}. The only systems of intransitivity of this subgroup G_1, which are not excluded by the conditions stated on p. 15, are 81, 81, 81, 81, 15, 15, 15, 15. In order that the transitive constituents of degree 81 contain in their orders the factor 5, they must be primitive groups of degree 81 of order 81.5. Consider the invariant subgroup H of G_1 corresponding to identity in a transitive constituent of degree 81. It follows from Theor. 6 that the degree of H cannot exceed 60. As G_1 could contain no other similar subgroup, the order of G_1 would be 81.5. The primitive group of degree 385 of order $3^4.5^2.7.11$ then contains 324.77 substitutions of order 5 of degree less than 385. By Sylow's theorem, a group of order $3^4.5^2.7.11$ cannot contain more than 11.81 subgroups of order 5^2. As this number of subgroups contains less than 324.77 substitutions, we have arrived at an absurdity.

G^{235}.

$S_1 = 117, 117.$
$S_2 = 39, 39, \ldots, 39.$
$S_3 = 13, 13, \ldots, 13, 39, 39, 39, 39.$
$S_4 = 13, 13, \ldots, 13, 39, 39.$
$S_5 = 13, 13, \ldots, 13.$
$S_6 =$ any set of systems of which some contain 9 letters.

The order of G^{235} would be of the form $5.47.3^{\alpha}.13^{\beta}$. Let $p = 47$ in Cor. 2, §1, and it follows that G^{235} does not exist.

This completes the determination of the primitive groups of odd order of degree less than 243. The results may be summarized as follows:

Aside from the invariant subgroups of the metacyclic groups there are only ten primitive groups of odd order of degree less than 243. The following list of

numbers gives the orders of these groups, the first factor as they are written being the degree of the group of the given order:* 25.3, 27.13, 27.39, 81.5, 121.3, 121.15, 125.31, 125.93, 169.7, 169.21.

Each of these groups is solvable. The following theorem may then be stated:

THEOREM 13.—*A simple group of odd composite order cannot be of degree less than* 243.

CORNELL UNIVERSITY.

* For the first four groups, see Burnside, Proc. Lond. Math. Soc., Vol. 33, pp. 178–185.